Schritt fuer Schritt zum Cisco SMB IP Communication System

Michael Salat
msalat@cisco.com

© 2004 Cisco Systems, Inc. All rights reserved.

SMB Top of Mind

AND do all that with limited staff and budget?

How do I protect my assets?

How can we be more productive?

How can I increase my profitability?

How can I be more adaptive?

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

The Network Role in SMB

AND do all that with limited staff and budget?

PROTECTED

COLLABORATIVE

CONNECTED

RESPONSIVE

© 2004 Cisco Systems, Inc. All rights reserved.

Cisco Confidential

Cisco's SMB Class Solutions

Intelligent Services Blueprints

Software Platforms

Security

Mobility

Telephony

Security | Availability | Quality of Service

Intelligent Switching

Integrated Services Routing

Wireless

Intelligent SP WAN

Cisco IOS SOFTWARE

Ease of Use/ Manageability

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Ausgangssituation

© 2008 Cisco Systems, Inc. All rights reserved.

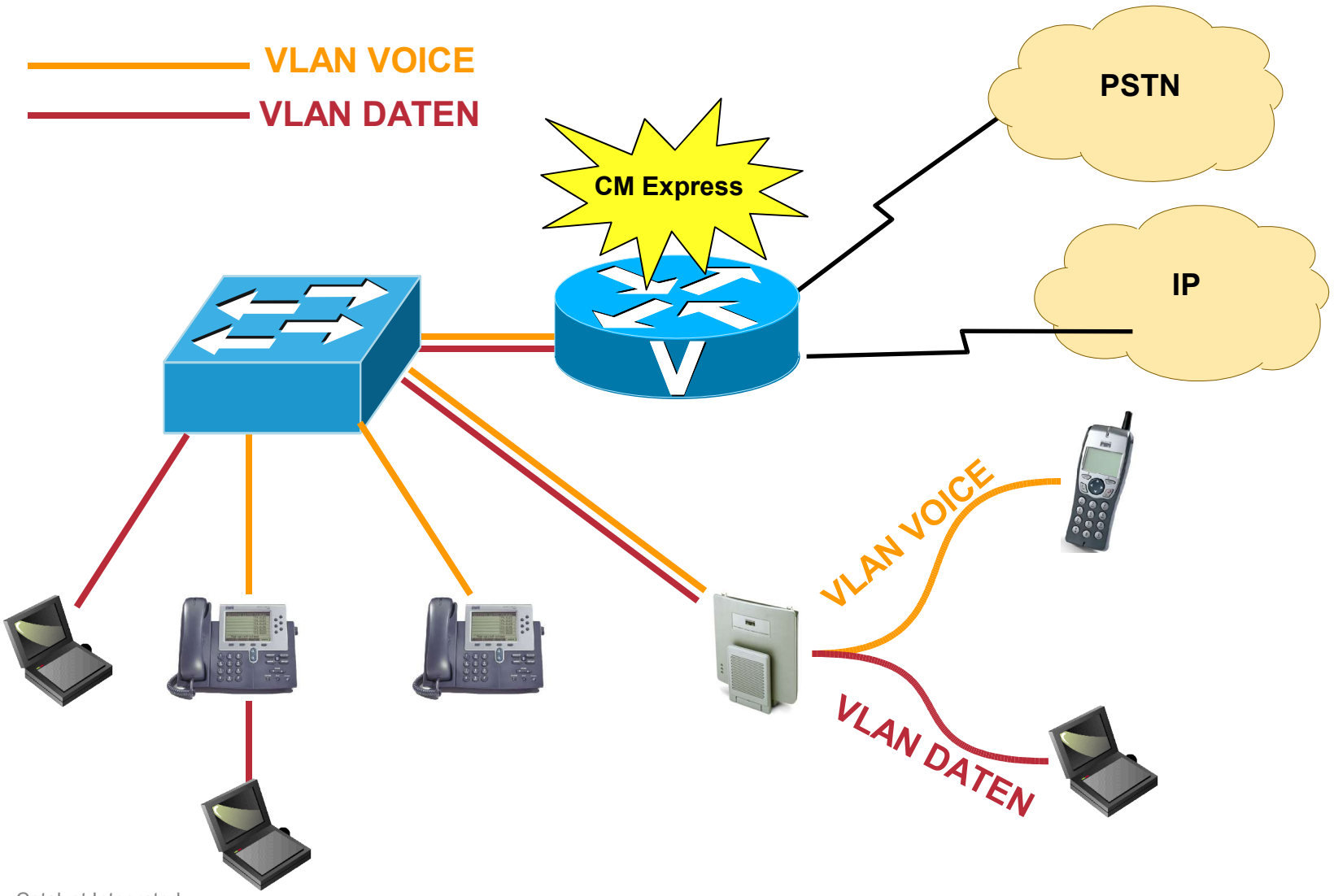
Typisches SMB Netzwerk

- Switches: Cisco, HP, 3Com, D-Link, Netgear,…
- Router: Cisco, HP, 3Com, Bintec, Zyxel,…
- Security: Cisco, A/V SW, Firewall (Linux, SW / appliance),…
- WLAN: Cisco, Symbol, D-Link, Netgear,…
- Telefonie: Cisco, Alcatel, Tenovis, Siemens,…

- Strategische Bedeutung des Netzwerk meist nicht gegeben, nur Kostfaktor
- HETEROGEN, Management kostenintensiv
- PREISSENSITIV bei der Anschaffung
- Keine Betrachtung Anschaffungskosten vs. Gesamtzeit
  zB. Tiefkuehltruhe, C vs A++ Energieeff., mind. 10 Jahre
- Finanzierung meist ueber Kauf

© 2004 Cisco Systems, Inc. All rights reserved.

Cisco SMB IP Communication system

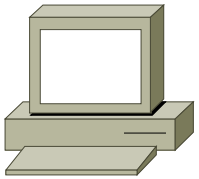


© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

LAN Switching Infrastruktur – Verbesserung der internen Sicherheit

© 2003 Cisco Systems, Inc. All rights reserved.

Apply Authentication Model to the Network – use 802.1x

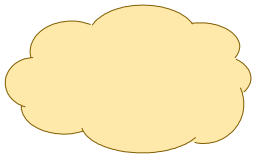


I'd like to connect to the network

Do you have identification?

Yes, I do. Here it is.

Thank you. Here you go.

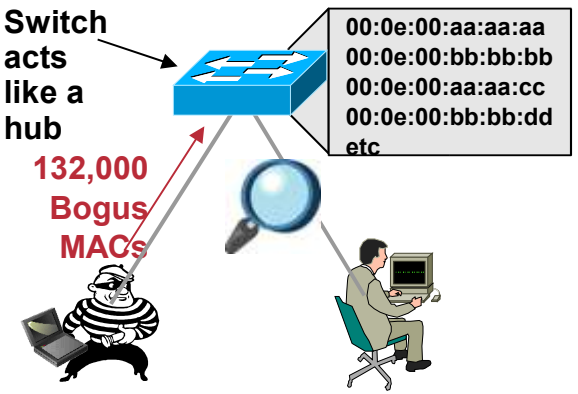


© 2004 Cisco Systems, Inc. All rights reserved.

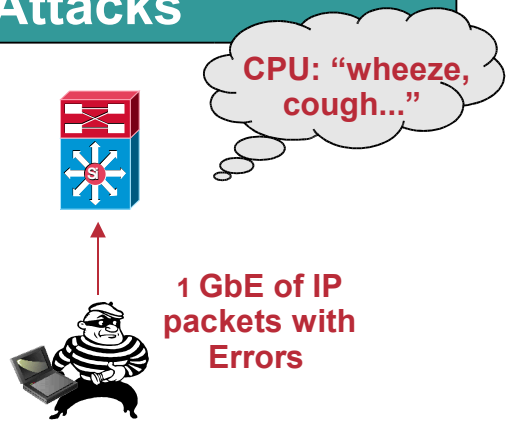
LAN Security Threats

Cisco.com

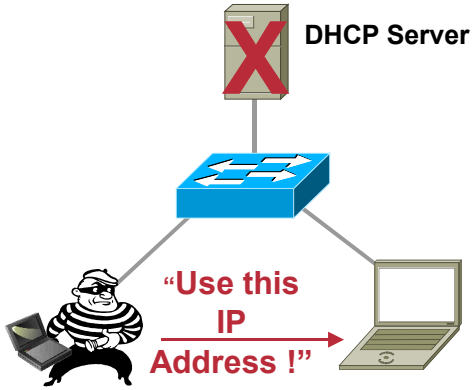
MAC Flooding Attacks



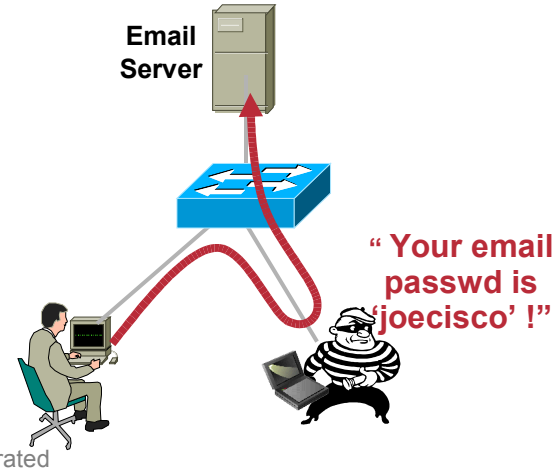
Network Element Attacks



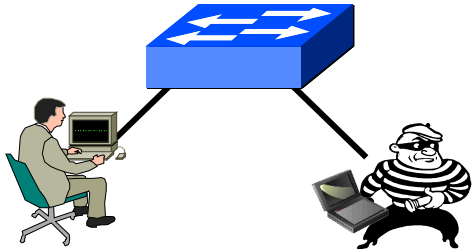
DHCP Vulnerabilities



Man-in-the-Middle Attacks



Host Spoofing Attacks



© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

LAN Security Threats

Targeted by the Catalyst Integrated Security Features

- **VLAN Hopping Attack**
- **Spanning Tree Attack**
- **MAC Address Flooding Attack**
  - SYN floods with random src and dst MAC, random src and dst IP
  - After CAM Table Fills, Traffic Flooding Occurs (32K entries)
  - Random IP addresses include multicast address space and will eventually cause distribution layer to fail due to excessive processing of multicast routes
- **DHCP Rogue Server Attack**
  - Hacking Tool: gobbler or actual rogue DHCP server
    - Man in the middle attacks via DNS or IP default GW forging
- **DHCP Starvation**
  - Hacking Tool: gobbler
    - Depletion of DHCP address space
- **ARP Spoofing or ARP Poisoning Attack**
  - Hacking Tool: ettercap, dsniff, arpspoof
    - Menu driven discovery of MAC level topology with ARPs and DNS Reverse Name Lookup
    - Man in the middle attacks with integrated packet capture and password sniffing

© 2004 Cisco Systems, Inc. All rights reserved.

Dsniff—A Collection of Tools to Do

- ARP spoofing
- MAC flooding
- Selective sniffing
- SSH/SSL interception

Dug Song, Author of dsniff

www.monkey.org/~dugsong/dsniff

© 2004 Cisco Systems, Inc. All rights reserved.

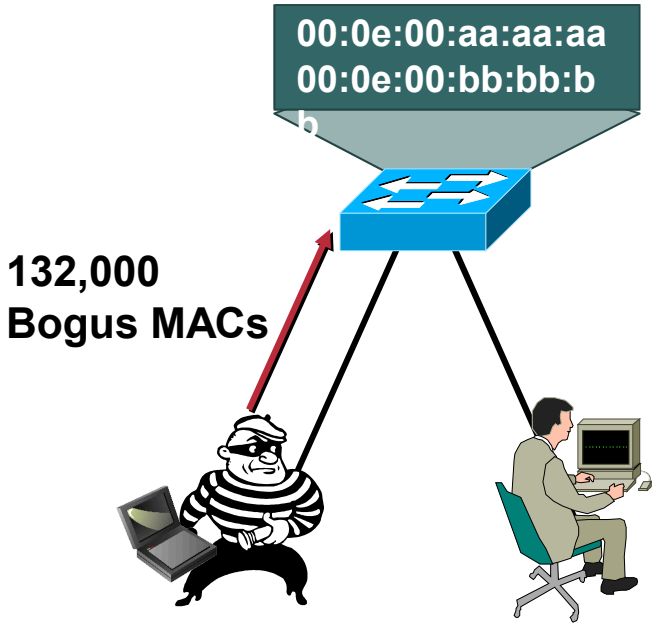
Windows Plattformen

- Kain und Abel
- Runterladen und selbst ausprobieren
- Beim Kunden im LAN die Verletzbarkeit aufzeigen

© 2004 Cisco Systems, Inc. All rights reserved.

Raising the Bar on Surveillance Attacks

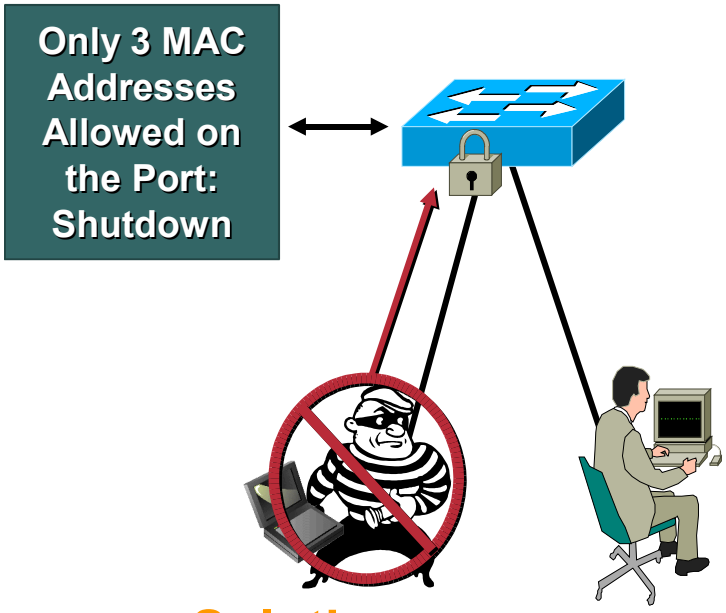
MAC-Based Attacks



Problem:

"Script Kiddie" Hacking Tools Enable Attackers Flood Switch CAM Tables with Bogus Macs; Turning the VLAN into a "Hub" and Eliminating Privacy

Switch CAM Table Limit is Finite Number of Mac Addresses



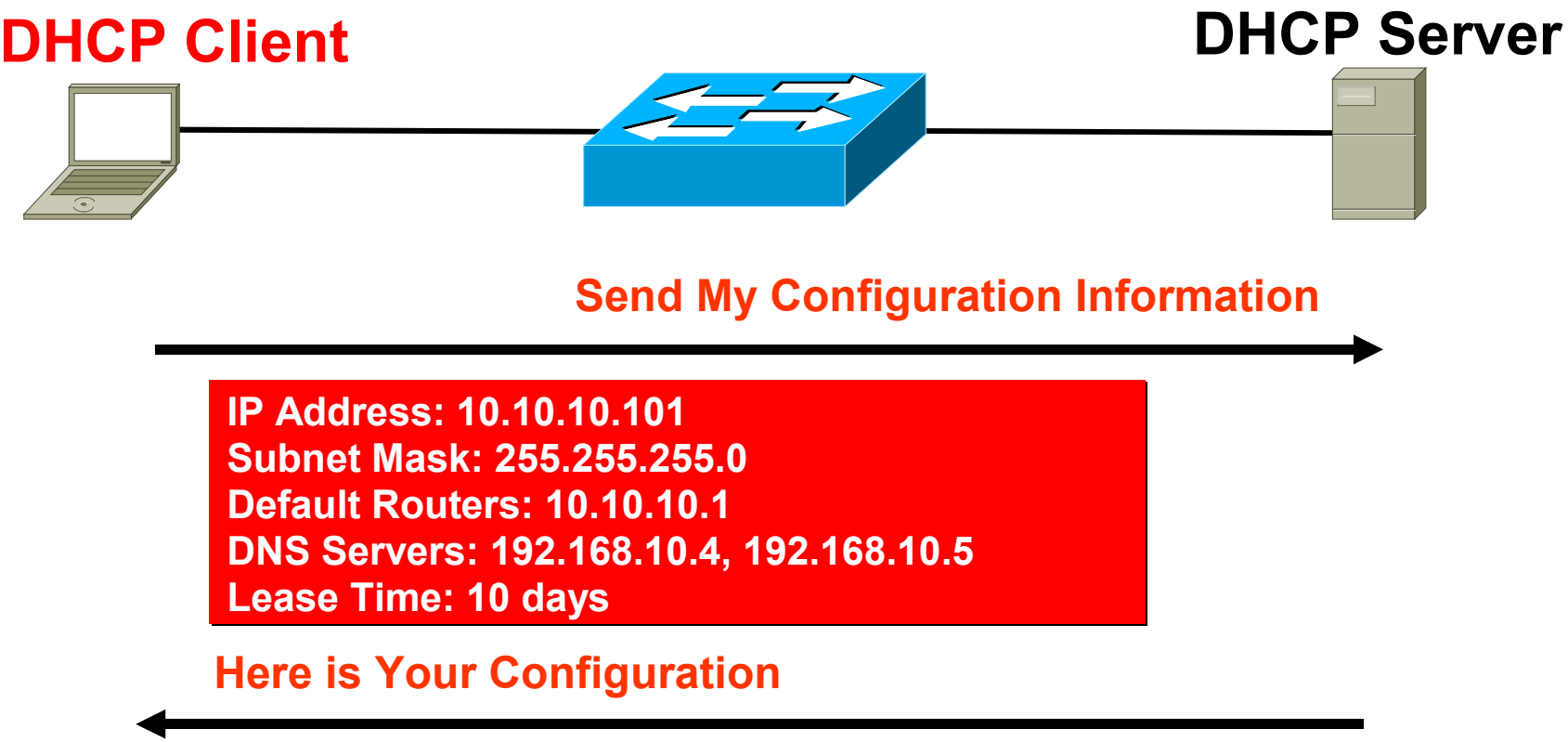
Solution:

Port Security Limits MAC Flooding Attack and Locks down Port and Sends an SNMP Trap

© 2004 Cisco Systems, Inc. All rights reserved.

DHCP Function

High Level Function

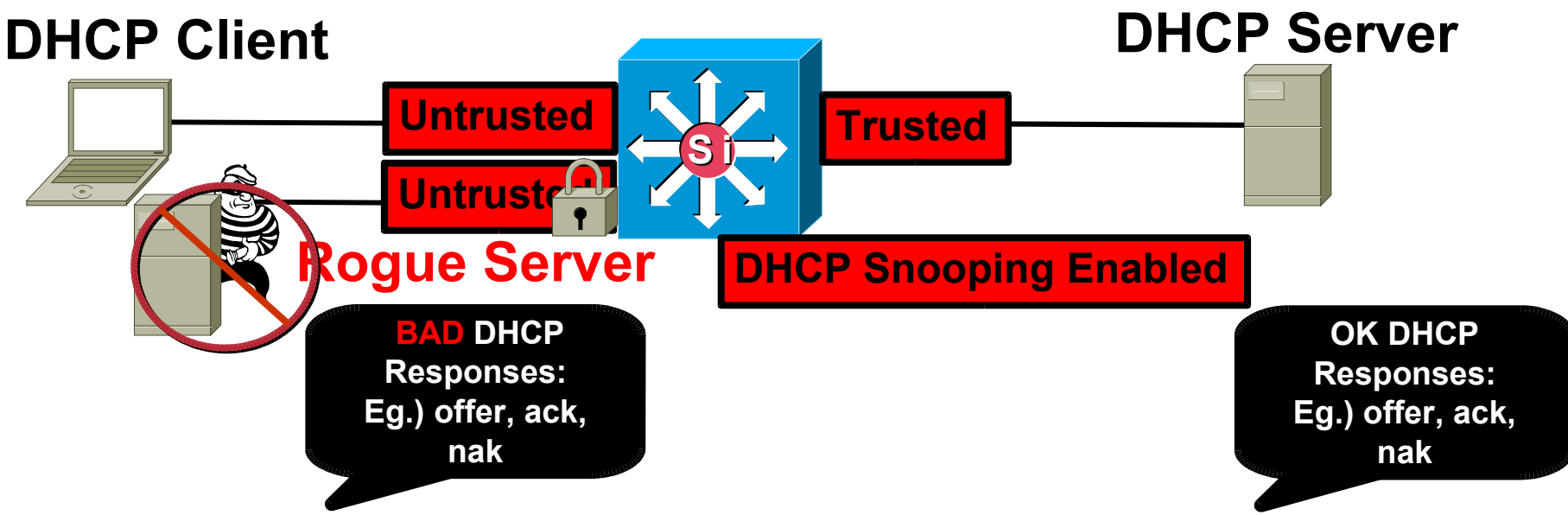


- Server dynamically assigns IP address on demand
- Administrator creates pools of addresses available for assignment
- Address is assigned with lease time
- DHCP delivers other configuration information in *options*

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

DHCP Snooping

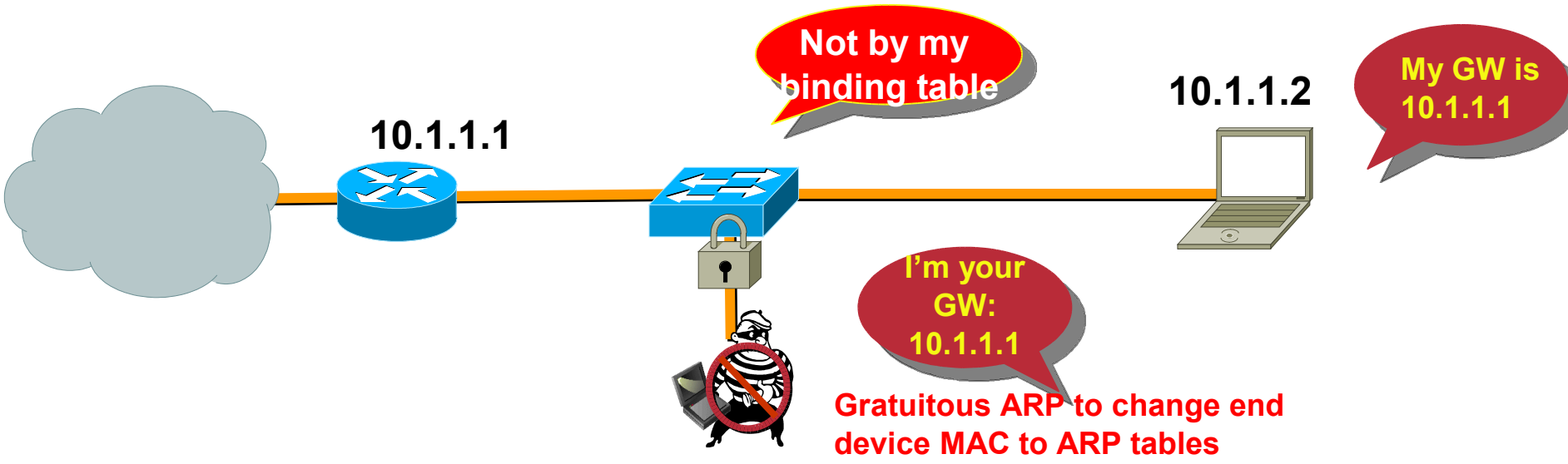
Prevents Rogue Server and Limits DHCP DoS



- **Prevents MiM and limits denial of service (DoS) attacks based on DHCP protocol**
  - **Malicious—user pretends to be the Network DHCP Server to reply with DNS or GW info to redirect traffic OR user pretends to be multiple DHCP clients to starve the DHCP address pool**
  - **Misconfiguration—user configures router (DHCP server) incorrectly**
- **How it works:**
  - **For DHCP packets originating from untrusted ports (client ports), DHCP Snooping drops all DHCP OFFER, ACK, NACK, or nonzero giaddr packes (server oriented packets). DHCP Snooping forwards DHCP client requests from untrusted ports and builds a DHCP binding table.**
  - **If DHCP server is not local to the Catalyst Switch, trust the uplink port**

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Dynamic ARP Inspection



- A binding table containing IP-address and MAC-address associations is dynamically populated using DHCP Snooping
- Can also use ARP ACLs to deny (and optionally log) all invalid IP/MAC binding attempts for non-DHCP assigned IP Addresses
- Private VLAN support coming.
- Prevents attacks that use ARP with an IP not in the binding table in the switch

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

802.1x Component Availability

	802.1x basic	802.1x Voice-VLAN	802.1x Vlan Asign	801.1x Guest VLAN	802.1x Port Security
C6500 CatOS					
C6500 IOS		CY2005		CY2005	CY2005
C4500 CatOS (EoS)					
C4500 IOS					
C3750					
C3550					
C2950 EI					
C2950 SI					

available future not planned

© 2004 Cisco Systems, Inc. All rights reserved.

Catalyst Security Features

	Port Security	DHCP snooping	DAI dyn. ARP inspect.	IP source guard	802.1x Auth.
C6500 CatOS					
C6500 IOS		H2/2005	H2/2005	H2/2005	
C4500 CatOS (EoS)					
C4500 IOS					
C3750			SMI !!	SMI !!	
C3560			SMI !!	MI !!	
C3550			SMI !!	SMI !!	
C2950 EI					
C2950 SI					

available future not planned

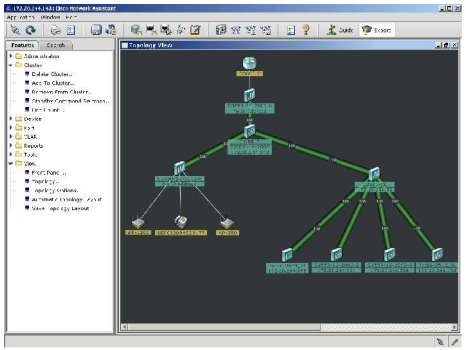
© 2004 Cisco Systems, Inc. All rights reserved.

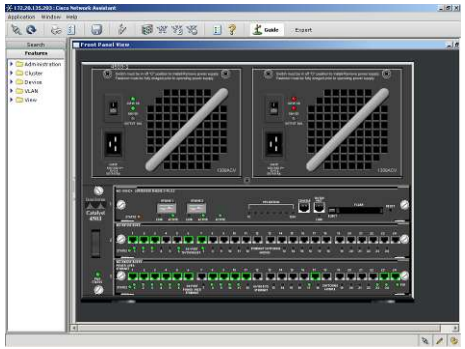
Cisco Network Assistant addresses the needs of both users and resellers

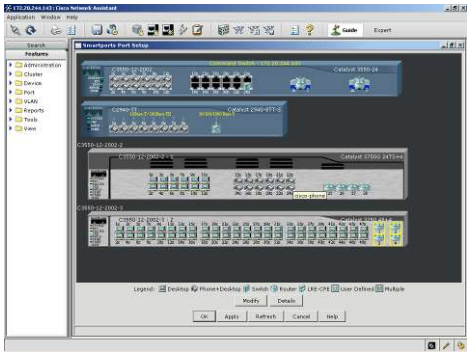
FREE!!

Cisco.com

www.cisco.com/go/networkassistant







Single Point of Management

- Auto discovery of Cisco devices: Switches, Routers, Access Points and IP Phones
- Displays physical network topology
- Launch point for other embedded Cisco device managers

Easy and Accurate Configuration

- Offers configuration tools & wizards
- Take advantage of proven Cisco Best Practices with no Cisco IOS knowledge

Simplified Network Health Checking

- Easy updating of IOS-based switch software images
- Real time reporting and inventory information

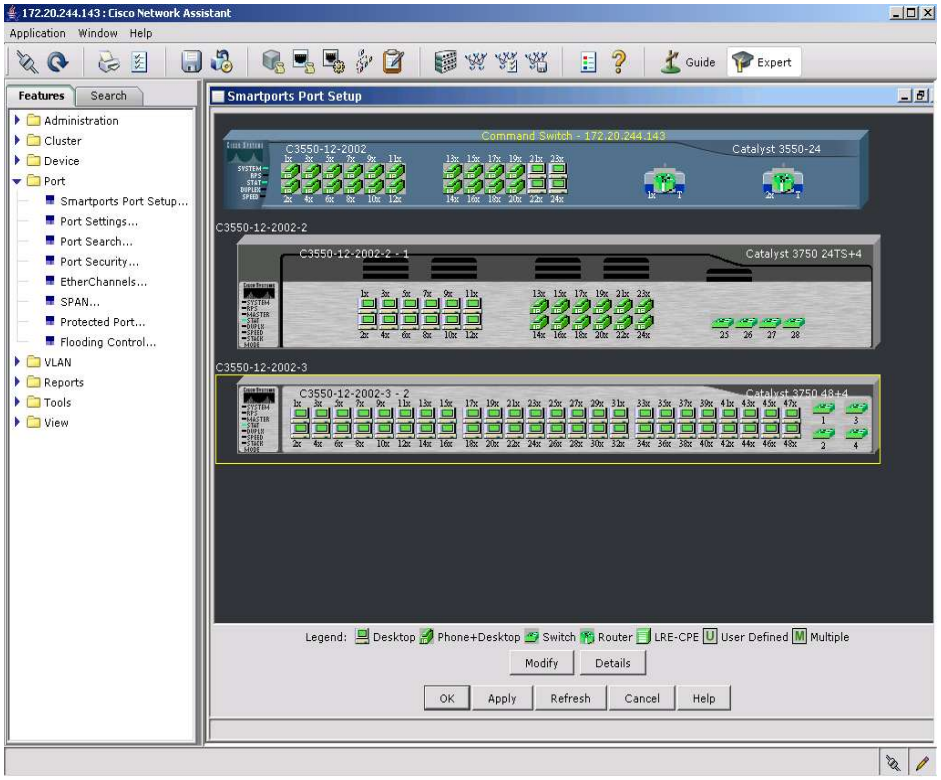
Simplified Troubleshooting Assistance

- Troubleshooting tools
- Single view of network for health status
- Integrated with Cisco.com for automated application updates

© 2004 Cisco Systems, Inc. All rights reserved.

Easy and Accurate Configuration

- **Smartports: Easy and accurate configuration of Catalyst features**
- **Offers Security and Voice/Video deployment wizards**
- **Offers management of Cisco SMB switch offerings (Catalyst 2xxx, 3xxx and 4xxx)**
- **Benefits:**
  - **Extract maximal value from a Cisco SMB network**
  - **Helps accelerate advanced technology deployments**
  - **Take advantage of proven Cisco Best Practices with minimal Cisco IOS knowledge**



© 2004 Cisco Systems, Inc. All rights reserved.

Smartports

From this:

Global Commands

```
failureerrdisable recovery cause link-flap
errdisable recovery cause udld
errdisable recovery interval 60
vtp domain [smartports]
vtp mode transparent
udld aggressive
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
```

Interface Commands

```
default interface range FastEthernet[1]/0/[1 - 48]
interface range FastEthernet[1]/0/[1 - 48]
switchport access vlan [data]
switchport mode access
switchport voice vlan [voice]
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
auto qos voip cisco-phone
spanning-tree portfast
spanning-tree bpduguard enable
```

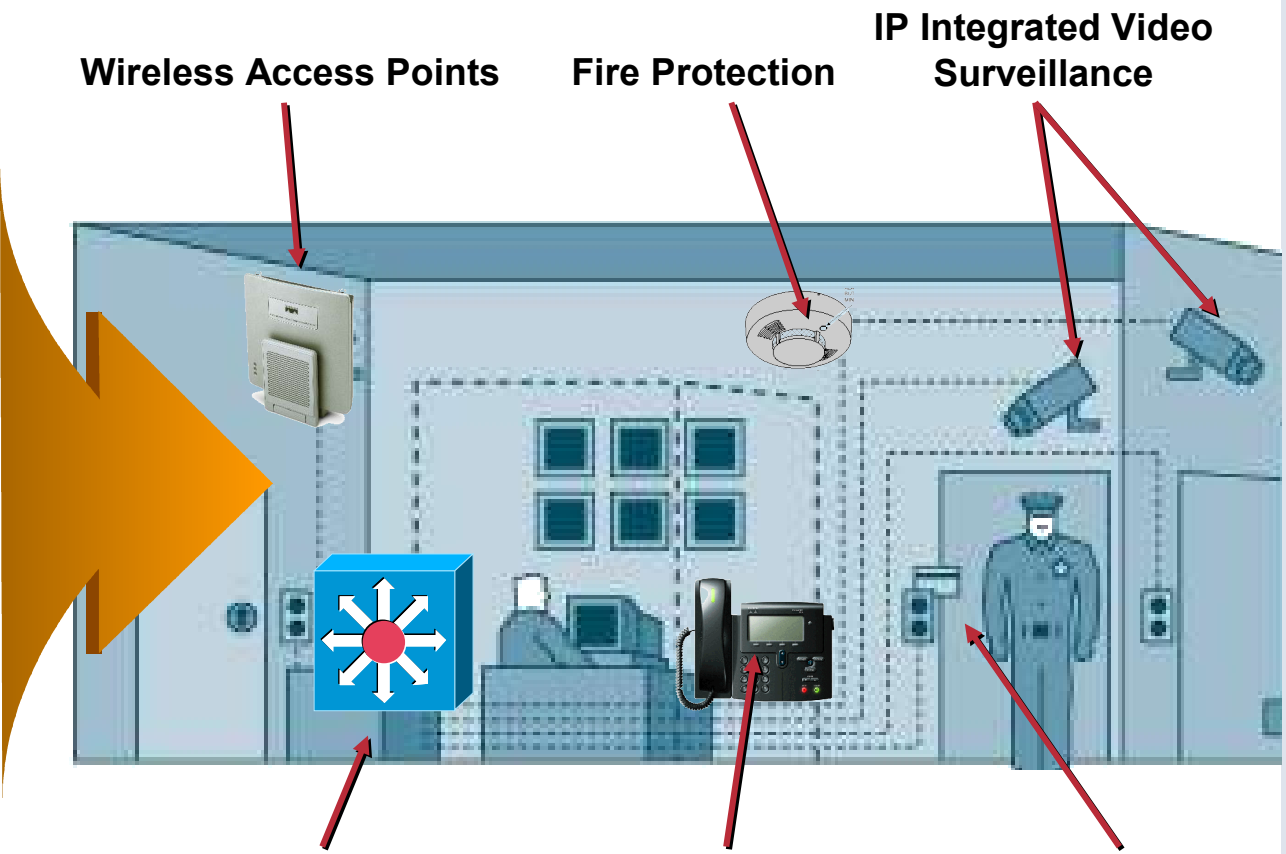
To this:

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

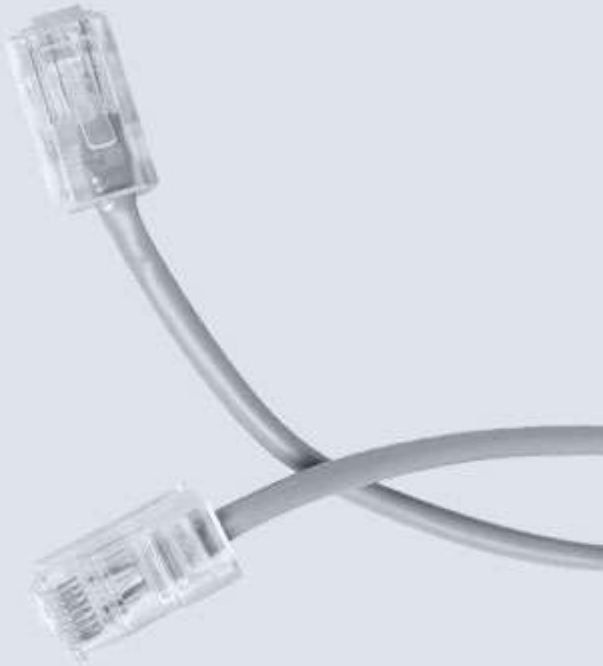
A Glimpse into the Future…

The Ethernet Powered Organization

Cisco.com



Power over Ethernet (PoE) Delivers 48V DC Power over a Standard Copper Ethernet Cable



The Power and Network Is Used by the Connected Devices for Their Operation

© 2004 Cisco Systems, Inc. All rights reserved.

Cisco Confidential

Cisco Catalyst 4500 Series Chassis Specs

	Catalyst 4503	Catalyst 4506	Catalyst 4507R	Catalyst 4510R
Sup Redundancy	n/a	n/a	Yes	Yes
Slots	3	6	7	10
Ports (max) + GE	96+2	240+2	240+4 (Sup5)	380+ 2 10GE
Dimensions (RUs)	7	10	11	14
Power Supplies	1+1	1+1	1+1	1+1
Supervisors	Sup2 – Sup5	Sup2 – Sup5	Sup2+,4,5	Sup5

© 2004

Catalyst 4503 Series SMB Solution

Introducing Supervisor II-Plus-TS

New for SMB

- **Designed specifically for SMB Networks and Enterprise Branch offices**
- **Increases Catalyst 4503 maximum port density to 116 total ports**
- **12 wire speed 10/100/1000 ports with PoE and 8 SFP ports built in on the front faceplate of the Supervisor**
- **Two available line card slots compatible with all Catalyst 4500 Series line cards**

- **Cisco IOS based Layer 2 Supervisor with Layer 3 & Layer 4 services exclusively for the Catalyst 4503**
- **Based on Catalyst 4500 Supervisor II-Plus Hardware and Software**
- **Faceplate ports have many uses including PoE device connections, server connections, uplinks, gigabit aggregation or user ports**

New

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Catalyst 4503 Supervisor II-Plus-TS Specifications

- Catalyst 4503 Only
- 64 Gbps Switching Capacity, 48 Million packets-per-second forwarding rate
- Support for Jumbo Frames on all non-blocking GE ports (including 10/100/1000 faceplate ports)
- Extensive Wire Rate Security and QoS Features
- Support for 32K MAC Addresses
- Support for 4K VLANs
- 802.1Q VLAN Tagging on all ports
- RIP v1, v2 and Static Routes
- 32K IPv4 FIB unicast and multicast forwarding entries
- (IOS 12.2(20)EWA or later)

© 2004 Cisco Systems, Inc. All rights reserved.

Catalyst 3750 – Cisco StackWise Technology

- 32 Gbps stack interconnect
- Stack up to 9 units
- Separate stacking port
- 1:N master redundancy
- Autoconfiguration and Cisco IOS version check/update
- Cross-stack EtherChannel and QoS
- Line-speed performance with QoS and ACLs for gigabit Ethernet
- Hot add and delete of gigabit Ethernet and Fast Ethernet chassis in same stack
- Patented cable connector

Unified stacking, behaving as a single unit

© 2004 Cisco Systems, Inc. All rights reserved.

Cisco Catalyst 3750 Series Switches—Current Models

Catalyst 3750G-24T

- 24 10/100/1000 ports

Catalyst 3750G-24TS

- 24 10/100/1000 ports
- 4 SFP ports

Catalyst 3750G-12S

- 12 SFP GE ports

Catalyst 3750-24

- 24 10/100 ports
- 2 SFP ports

Catalyst 3750-48

- 48 10/100 ports
- 4 SFP ports

Two Software Versions

Standard Multilayer Software Image (SMI)

- Enterprise-class intelligent services: advanced QoS, security, high availability, routed ACLs, HSRP, RIP, and static IP routing

Enhanced Multilayer Software Image (EMI)

- SMI feature set plus: dynamic IP unicast routing, smart multicast routing, Policy Based Routing, Advanced Security features

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Cisco Catalyst 3560 Series Model Overview
Fast Ethernet Models

Cisco.com

Catalyst 3560-24TS

- 24 10/100 ports
- 2 SFP ports

Catalyst 3560-48TS

- 48 10/100 ports
- 4 SFP ports

Catalyst 3560-24PS

- 24 10/100 ports
- 2 SFP ports
- 370W IEEE 802.3af / Cisco prestandard PoE

Catalyst 3560-48PS

- 48 10/100/1000 ports
- 4 SFP ports
- 370W IEEE 802.3af / Cisco prestandard PoE

Two Software Versions

- **Standard Multilayer Software Image (SMI)**

  Enterprise-class intelligent services: Advanced QoS, enhanced security, high availability, static and Routing Information Protocol (RIP) IP routing

- **Enhanced Multilayer Software Image (EMI)**

  SMI feature set plus: Advanced hardware-based IP unicast and multicast routing, and policy-based routing (PBR)

- **Orderable with either software image**

- **Upgrade license available**

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Cisco Catalyst 3560 Series Model Overview
Gigabit Ethernet Models

Catalyst 3560G-24TS

NEW

- 24 10/100/1000 ports
- 4 SFP ports

Catalyst 3560G-48TS

NEW

- 48 10/100/1000 ports
- 4 SFP ports

Catalyst 3560G-24PS

NEW

- 24 10/100/1000 ports
- 4 SFP ports
- 370W IEEE 802.3af / Cisco prestandard PoE

Catalyst 3560G-48PS

NEW

- 48 10/100/1000 ports
- 4 SFP ports
- 370W IEEE 802.3af / Cisco prestandard PoE

Two Software Versions

- **Standard Multilayer Software Image (SMI)**

  Enterprise-class intelligent services: Advanced QoS, enhanced security, high availability, static and Routing Information Protocol (RIP) IP routing

- **Enhanced Multilayer Software Image (EMI)**

  SMI feature set plus: Advanced hardware-based IP unicast and multicast routing, and policy-based routing (PBR)

- **Orderable with either software image**

- **Upgrade license available**

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Catalyst 2950 Series

Cisco.com

Flexible Uplinks

Advanced Intelligent Features / Enhanced Image

Catalyst 2950G-12-EI

12 10/100 Ports
2 GBIC Ports

Catalyst 2950G-24-EI

24 10/100 Ports
2 GBIC Ports

Catalyst 2950G-24-EI-DC

24 10/100 Ports
2 GBIC Ports

Catalyst 2950G-48-EI

48 10/100 Ports
2 GBIC Ports

Fixed Uplinks

Basic Cisco IOS® Features /Standard Image

Catalyst 2950-12

12 10/100 Ports

Catalyst 2950-24

24 10/100 Ports

Catalyst 2950T-48

New!

48 10/100 Ports 2 fixed 10/100/1000BASE-T port

Catalyst 2950SX-24

24 10/100 Ports 2 fixed 1000BASE-SX ports

Catalyst 2950SX-48

New!

48 10/100 Ports 2 fixed 1000BASE-SX ports

Catalyst 2950T-24

24 10/100 Ports
2 fixed 10/100/1000BASE-T ports

Catalyst 2950C-24

24 10/100 Ports
2 fixed 100BASE-FX ports

© 2004 Cisco Systems, Inc. All rights reserved.

Fuer die Zukunft geruestet…

- QoS
- VoiceVLANs
- SW Upgradeable fuer lange Nutzung

© 2004 Cisco Systems, Inc. All rights reserved.

Sales Tool…

- TradeIn Mitbewerb Switches: 3Com, HP, Nortel,…
- TradeIn Cisco alt (Hub/Switch) vs. Cisco neu
- SMB Neukunden: Icebreaker Promo (Preissupport)
- PLUS -> OIP Programm (+6% von Listpreis)

© 2004 Cisco Systems, Inc. All rights reserved.

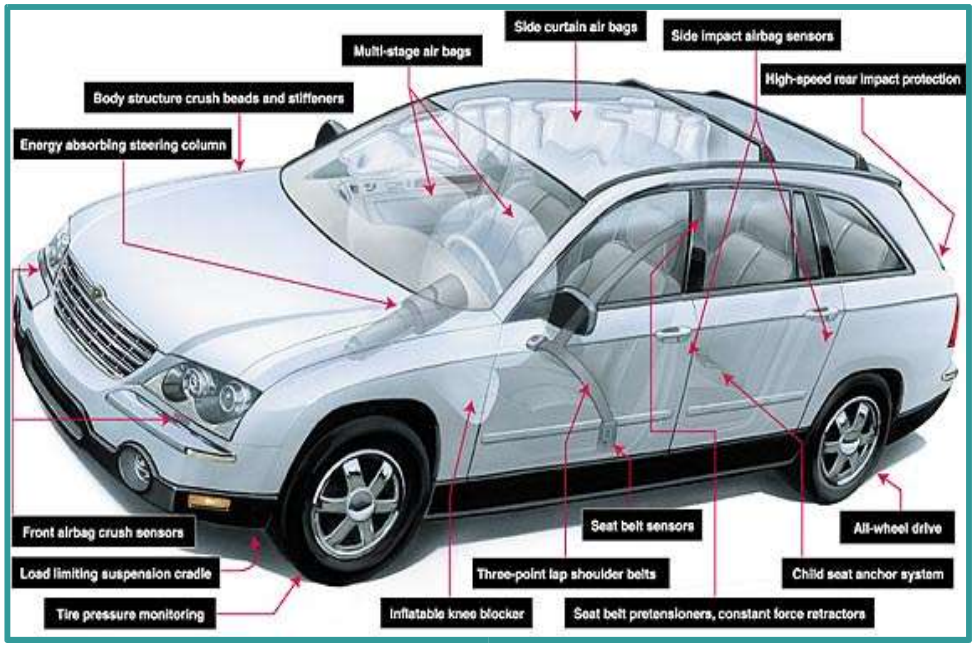
Sichere Kommunikation nach aussen – Router Security & VPN

© 2003 Cisco Systems, Inc. All rights reserved.

Self-Defending Integrated Security Systems

Security is not Optional!

Cisco.com



Security as an Option

- Security is an add-on
- Challenging integration
- Not cost effective
- Cannot focus on core priority

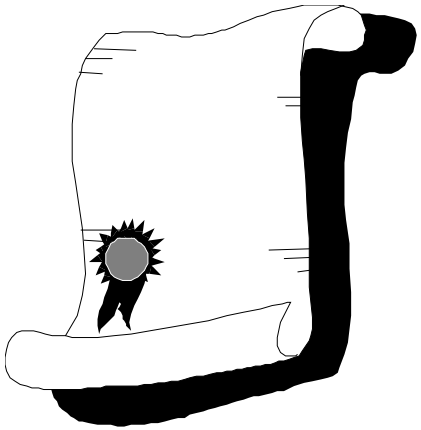
Security as part of a System

- Security is built-in
- Intelligent collaboration
- Appropriate security
- Direct focus on core priority

© 2004 Cisco Systems, Inc. All rights reserved.

What Is a Security Policy?

"A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide."



RFC 2196, Site Security Handbook

© 2004 Cisco Systems, Inc. All rights reserved.

Why Create a Security Policy?

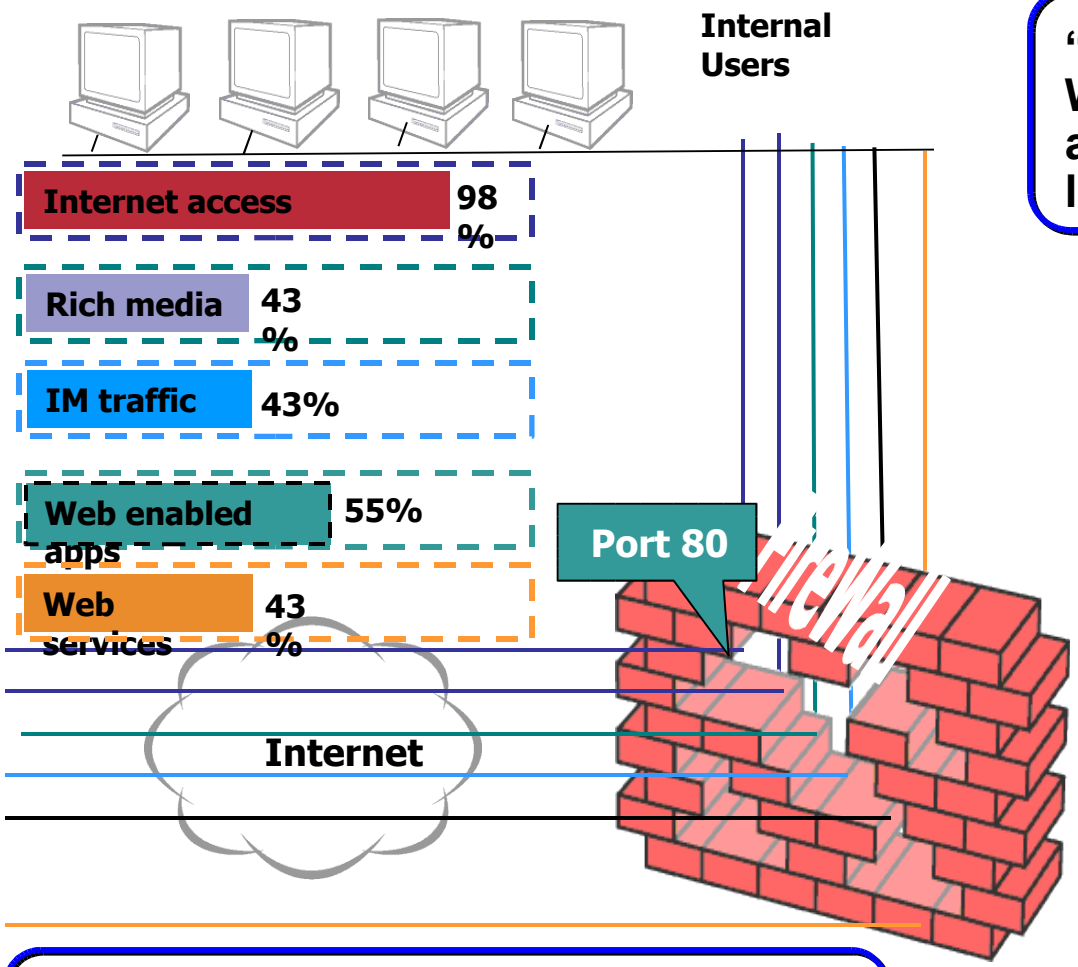
- To create a baseline of your current security
- To set the framework for security implementation
- To define allowed and not allowed behaviors
- To help determine necessary tools and procedures
- To communicate consensus and define roles
- To define how to handle security incidents

© 2004 Cisco Systems, Inc. All rights reserved.

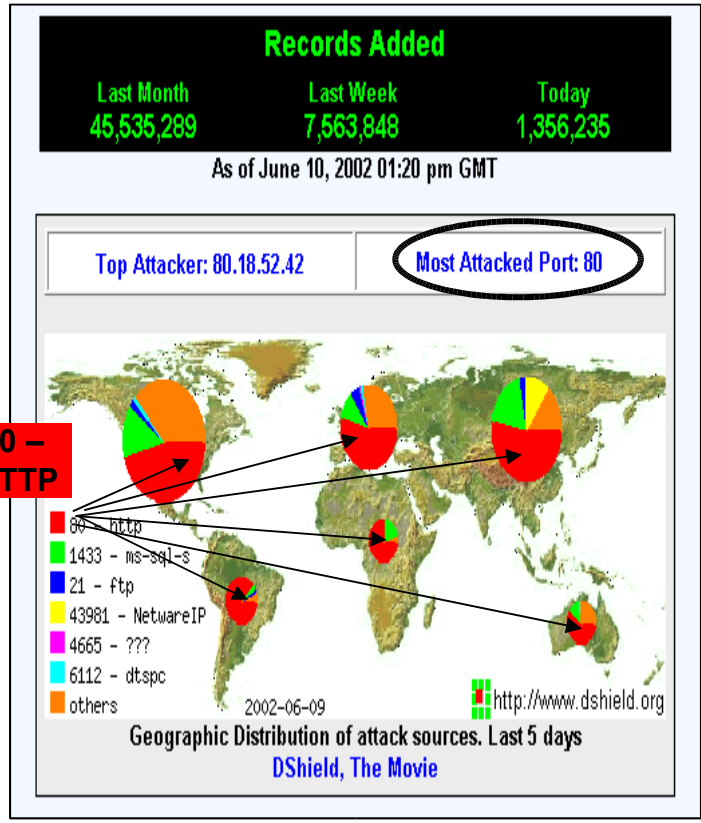
Companies Are Opening Port 80

Attacks Enter Through Web-enabled Applications

Cisco.com



"…75% of successful attacks against Web servers are entering through applications and not at the network level."



John Pescatore, VP and Research Director, Gartner, June 2002.

64% of enterprises have opened Port 80 on their firewalls for their growing web application traffic

Source: Aug 2002 InfoWorld/Network Computing survey of IT Professionals

Cisco IOS Firewall
Advanced Application Inspection and Control

Cisco.com

HTTP Inspection Engine

- Delivers application level control through inspection of port 80 tunneled traffic
  - Convergence of Cisco IOS Firewall and Inline IPS technologies
- Control port 80 misuse by rogue apps that hide traffic inside http to avoid scrutiny
  - Example: Instant messaging and peer-to-peer applications such as Kazaa

Email Inspection Engine

- Control misuse of email protocols
- SMTP, ESMTP, IMAP, POP inspection engines

Inspection Engines provide protocol anomaly detection services

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Cisco IOS IPS

New Features and Engines – All Inline!

- **Newly enhanced router-based IPS enables broadly-deployed worm and threat mitigation services -- even to remote branch offices**
- **String Engines enable custom matching of any string in the packet**
  - ***Customize signatures for quick reaction to new threats***
  - **TCP String, UDP String, ICMP String, Trend Micro**
- **400 worm and attack signatures added – more than 1200 total signatures from which to dynamically select**
- ***Supports Trend Micro Signatures***

© 2004 Cisco Systems, Inc. All rights reserved.

Cisco IOS Security Opportunities

- **Sell Security Bundles with every Cisco router!**
- **New Cisco IOS Security enhancements such as application inspection and additional Intrusion Prevention capabilities**

  Make sure each router sold contains -SEC/K9 or –HSEC/K9

  Upgrade customers' IOS version to include the new security features

© 2004 Cisco Systems, Inc. All rights reserved.

Security Device Manager
SDM Wizard Options

- **Overview**
  - View IOS version, hardware installed and configuration summary
- **LAN Configuration**
  - Configure the LAN interfaces and DHCP
- **WAN Configuration**
  - Configure PPP, Frame Relay, HDLC WAN interfaces
- **Firewall**
  - Two types of firewall wizard simple inside/outside or more complex inside/outside/DMZ with multiple interfaces.
- **VPN**
  - Three types of wizards to create a secure site-to-site VPN, Easy VPN and GRE tunnel with IPSec
- **Security Audit**
  - Perform a router security audit and provides easy instructions on how to lock down the insecure features found
- **Reset**
  - Restore to factory default settings.

© 2004 Cisco Systems, Inc. All rights reserved.

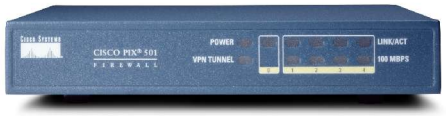
“They need security!"

Making Security Services Sales Faster, Easier: Cisco 3800, 2800 and 1800 Security Bundles

	Enhanced Security Bundles	Entry Security Bundles
3800 Series	Cisco 3825-HSEC/K9 Cisco 3845-HSEC/K9	Cisco 3825-SEC/K9 Cisco 3845-SEC/K9
2800 Series	Cisco 2801-HSEC/K9 Cisco 2811-HSEC/K9 Cisco 2821-HSEC/K9 Cisco 2851-HSEC/K9	Cisco 2801-SEC/K9 Cisco 2811-SEC/K9 Cisco 2821-SEC/K9 Cisco 2851-SEC/K9
1800 Series	Cisco 1841-HSEC/K9	Cisco 1841-SEC/K9
	Include: AIM-VPNII PLUS, Router, Cisco IOS Advanced IP Services	Include: Router, Cisco IOS Advanced Security

© 2004 Cisco Systems, Inc. All rights reserved.

Cisco PIX® 501 Firewall Overview

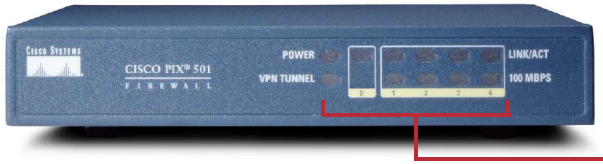


	Product Highlights
Enterprise-class Small / Home Office Security Appliance	• Robust stateful inspection firewalling • VPN for secure access to remote networks • Intrusion protection and much more…
Plug ‘n Play Small Office Networking	• Integrated 4-port 10/100 Mbps switch • Integrated DHCP client and server • Includes dynamic/static NAT and PAT support
Robust Remote Manageability	• Intuitive, web-based PIX Device Manager • Scaleable, multi-firewall management using Cisco Secure Policy Manager 3.0 • Supports other standards including telnet, SSH, TFTP, SNMP and syslog

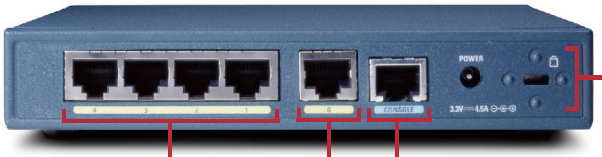
© 2004 Cisco Systems, Inc. All rights reserved.

Cisco PIX® 501 Firewall Hardware Overview

Front View



Rear View



Cisco IP Tel aware!

- Intuitive LEDs display current status of all network ports, power and VPN tunnels
- Integrated security lock slot provides improved physical security (cable lock not provided with unit)
- Console port for local PIX CLI access
- 10 BaseT port for outside interface
- Integrated 4-port 10/100 switch for inside “interface” with auto-sensing and auto-MDIX features

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

NEW! Cisco PIX Security Appliance Software v7.0

Cisco.com

Highlights

Over 50 major new features, across all major functional areas

Converging to common codebase with Catalyst 6500 Firewall Services Module

Timeframe

Beta program for all features – phase 1 started in Sept 2004

FCS target date – End of March 2005

Platforms Supported

Cisco PIX 515, 515E, 525 and 535 supported platforms

Catalyst 6500 Firewall Services Module release targeted for Q2CY05 (not EC)

Cisco PIX 501, 506, 506E support coming in a follow-on release*

Cisco PIX 520 not supported (PIX OS 6.3 last train for PIX 520)

System Requirements

PIX 515 and 515E will require a memory upgrade (128 MB RAM)

PIX 525 and 535 will not require any upgrades

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Cisco PIX Security Appliance Software v7.0

Advanced Web-Traffic Inspection Services

New in 7.0!

Cisco.com

New inspection services protect networks from web-based threats

- **Enterprise-class, advanced HTTP inspection services help protect from web-based attacks and other types of "port 80 misuse"**

  Includes customizable policies for detecting and blocking tunneled applications and attacks, including:

  - **Instant messaging applications (AIM, MSN Messenger, Yahoo)**
  - **Peer-to-peer applications (KaZaA)**
  - **And more!**

  Adds advanced TCP stream re-assembly and de-obfuscation engines for hidden attack detection

  Provides RFC compliance checking for protocol anomaly detection

  Supports HTTP command filtering for improved control and attack mitigation

- **Provides MIME type filtering and content validation capabilities**

  Control what types of content can traverse firewall

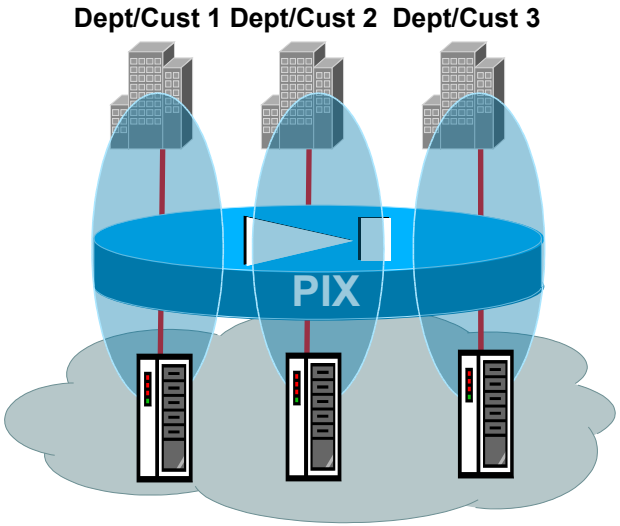
© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Virtualized Services and Transparent Operation

Simplifies Deployment and Reduces Operational Costs

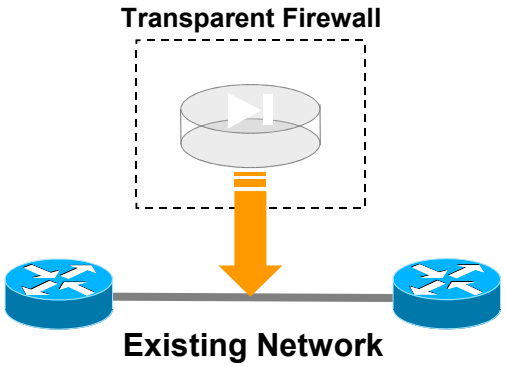
Scalable Security Services

- **Adds support for Security Contexts (virtual firewalls) to lower operational costs**
  - **Enables device consolidation and segmentation**
  - **Supports separated policies and administration**



Easy to Deploy Firewall Services

- **Introduces transparent firewall capabilities for rapid deployment of security**
  - **Drops into existing networks without need for readdressing the network**
  - **Simplifies deployments of internal firewalling and security zoning – new applications**



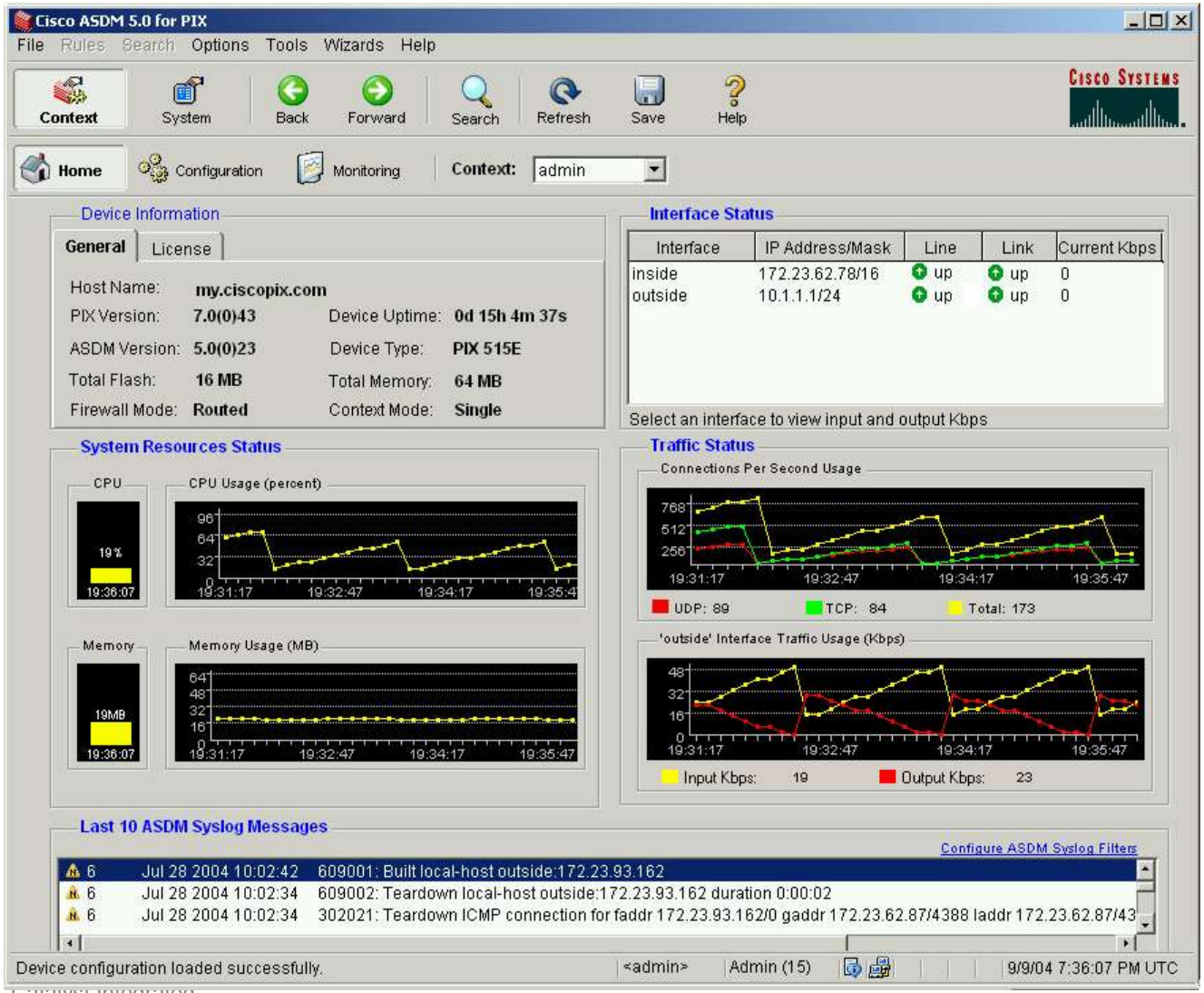
© 2004 Cisco Systems, Inc. All rights reserved.

Cisco Adaptive Security Device Manager v5.0

Next-Generation of Popular Cisco PIX Device Manager

New!

Cisco.com


Cisco ASDM 5.0 for PIX
File Rules Search Options Tools Wizards Help
Context System Back Forward Search Refresh Save Help
Cisco Systems
Home Configuration Monitoring Context: admin
Device Information
General License
Host Name: my.ciscopix.com
PIX Version: 7.0(0)43 Device Uptime: 0d 15h 4m 37s
ASDM Version: 5.0(0)23 Device Type: PIX 515E
Total Flash: 16 MB Total Memory: 64 MB
Firewall Mode: Routed Context Mode: Single
Interface Status
Interface IP Address/Mask Line Link Current Kbps
inside 172.23.62.78/16 up up 0
outside 10.1.1.1/24 up up 0
Select an interface to view input and output Kbps
System Resources Status
CPU
CPU Usage (percent)
19%
Memory
Memory Usage (MB)
19MB
Traffic Status
Connections Per Second Usage
UDP: 89 TCP: 84 Total: 173
'outside' Interface Traffic Usage (Kbps)
Input Kbps: 19 Output Kbps: 23
Last 10 ASDM Syslog Messages
Configure ASDM Syslog Filters
6 Jul 28 2004 10:02:42 609001: Built local-host outside:172.23.93.162
6 Jul 28 2004 10:02:34 609002: Teardown local-host outside:172.23.93.162 duration 0:00:02
6 Jul 28 2004 10:02:34 302021: Teardown ICMP connection for faddr 172.23.93.162/0 gaddr 172.23.62.87/4388 laddr 172.23.62.87/43
Device configuration loaded successfully.
<admin> Admin (15)
9/9/04 7:36:07 PM UTC

- Adds support for all major new features introduced in PIX OS v7.0
- Homepage includes new features, such as:
  - Platform uptime
  - Security Contexts
  - Real-time syslog viewer (last ten)
  - Improved navigation
  - Powerful search capabilities
  - And more!

© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Sales Tool…

- TradeIn Mitbewerb Security: Netscreen,Checkpoint
- TradeIn Cisco alt (Router) vs. Cisco neu (ISR Router)
- SMB Neukunden: Icebreaker Promo (Preissupport)
- PLUS -> OIP Programm (+6% von Listpreis)

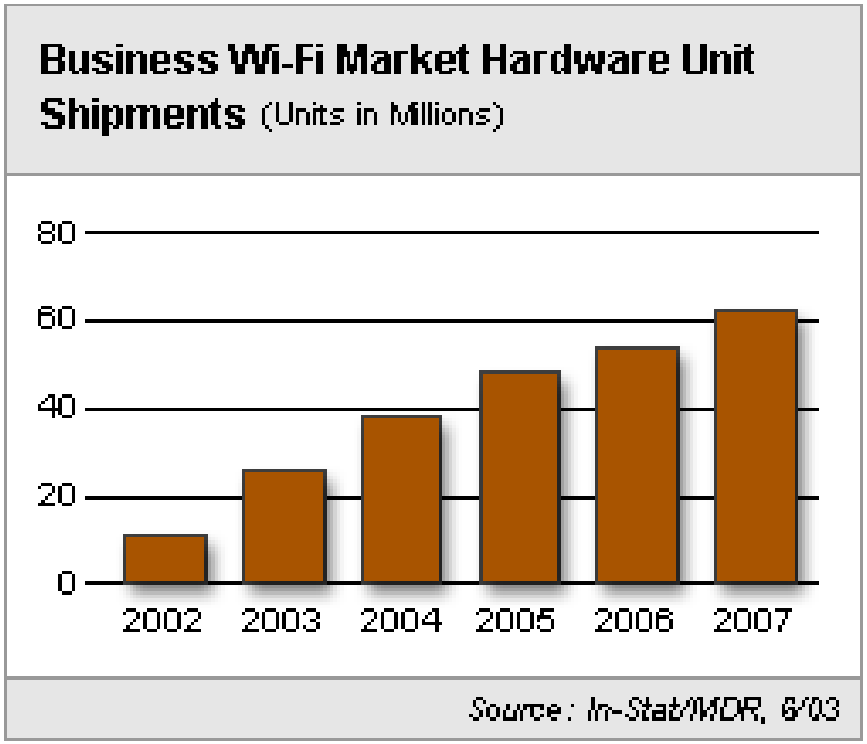
© 2004 Cisco Systems, Inc. All rights reserved.

Mobilitaet erhoehen – WLAN implementieren

© 2008 Cisco Systems, Inc. All rights reserved.

Forces Driving The Market

- 95% of notebook PC's shipped in 2005 will include Wi-Fi
- 113,555 World Wide Hotspots by the year 2006
- 50 million public hotspot users expected by 2005
- 74% of mobile workers will have VPN's by 2005
- Guest access will be a key requirement for enterprise networks
  - 30% of enterprise will implement by 2004
  - 60% by 2005/2006



© 2004 Cisco Systems, Inc. All rights reserved.

Cisco Compatible Program Status

Cisco.com

- **67 CCX Partners To Date**
  - Including 20 Wi-Fi Silicon Vendors
- **>150 Products Have Passed Cisco Compatible Testing**
  - Including laptops from HP, IBM, Dell, Toshiba, & Fujitsu
    - 6 of the top 8 laptop vendors in program
  - Form Factors: PC Card, PCI, USB, Barcode Scanners, etc.
  - >15M units Cisco Compatible products shipped to date
  - Many more 3rd party products in the CCX pipeline
- **CCX v2 Products are now hitting the market**
  - Enhanced Security
    - WPA
    - Interoperability testing for three 802.1X types
      - LEAP, PEAP, EAP-TLS
  - Mobility (Fast Secure Layer 2/3 Roaming)
  - Voice over WLAN features
  - Rogue AP Detection

All Intel Centrino™ Laptops are Cisco Compatible

http://www.cisco.com/en/US/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html

© 2004 Cisco Systems, Inc. All rights reserved.

Cisco Aironet Series Access Point Portfolio

Indoor Access Points

NEW!

Cisco Aironet 1130AG Series:
Dual band 802.11a/b/g enterprise-class AP with integrated antennas for easy deployment in offices and similar facilities

Cisco Aironet 1100 Series:
Single Band 802.11b/g enterprise-class AP with integrated antennas for easy deployment in offices and similar facilities

Indoor Rugged Access Points

NEW!

Cisco Aironet 1230AG Series:
Dual Band 802.11a/b/g enterprise-class AP with antenna connectors for flexible coverage capabilities in challenging RF environments

Cisco Aironet 1200 Series:
Single Band 802.11b/g enterprise-class AP that's upgradeable to dual band support with antenna connectors for flexible coverage capabilities in challenging RF environments

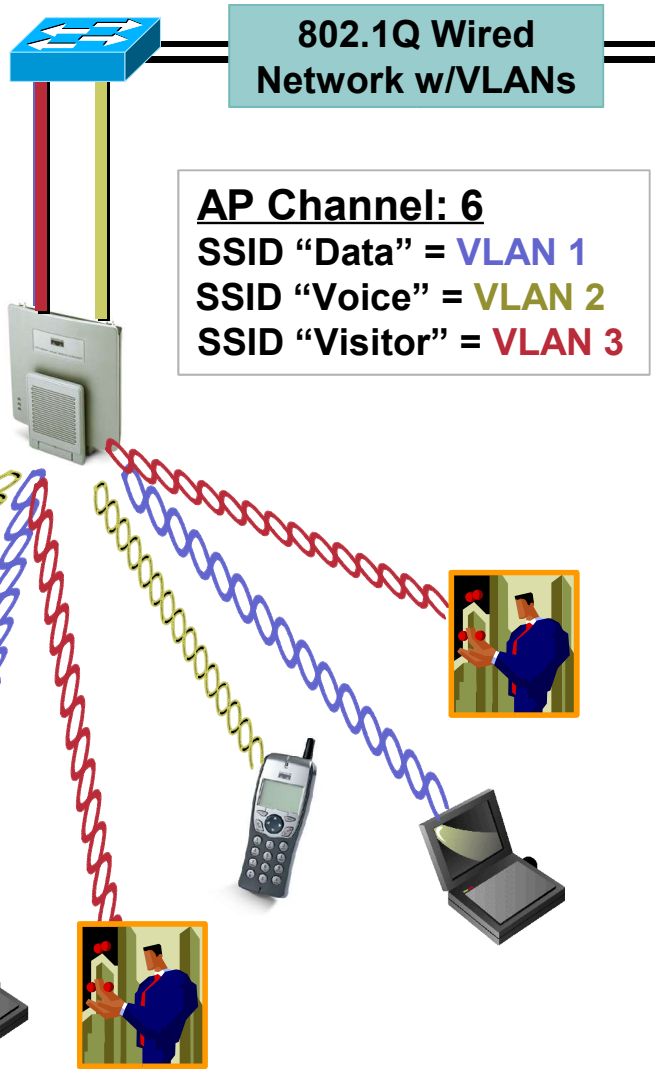
Outdoor Access Points/Bridges

Cisco Aironet 1300 Series:
Single Band 802.11b/g enterprise-class Outdoor AP/Bridge ideal for outdoor areas, network connections within a campus area, or outdoor infrastructure for mobile networks.

VLANs und QoS: For Security, Voice, Guest Access, etc.

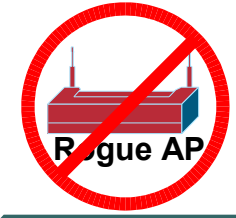
A Single WLAN Can Handle up to 16 Separate VLANs

By 2004, 30% of enterprises will implement Guest Access, rising to 60% by 2006. *-META Group, Sep.'03*



© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Solving the Rogue AP Problem



- **Step 1: Prevent**
  - Physical Security
    - Prevent unauthorized access to the bldg.
  - Develop a company-wide WLAN Policy
  - Install an IT-sanctioned WLAN
- **Step 2: Detect**
  - Intermittent checking with portable wireless sniffers
    - *AirMagnet, NetStumbler, Sniffer, WildPackets, etc.*
  - Continuous Monitoring with WLAN management tools
  - Engage AP's & Clients in the hunt
- **Step 3: Eliminate**
  - Rogue AP Suppression
    - Shut down its switch port from Network Operations Center
  - Locate the Rogue AP, and physically remove it

Primary Threat is From Inside

>99.9% of Rogue APs

Jones From Accounting

<.1% of Rogue APs

Harry the Hacker

"80%+ of enterprises experience exposure to rogue wireless networks"
-META Group, Aug.'03

© 2004 Cisco Systems, Inc. All rights reserved.

Datennetz und Telefonanlage integrieren

© 2003 Cisco Systems, Inc. All rights reserved.

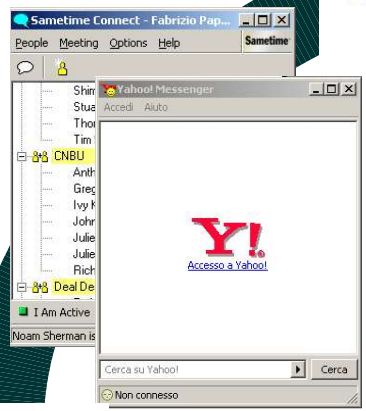
Today communication

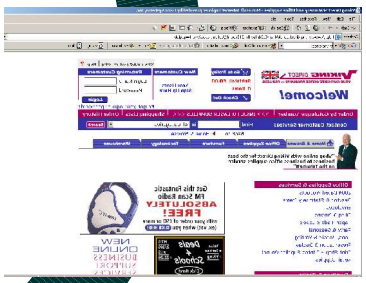
Wireless LANs

Mobile Phones

SW Upgrades

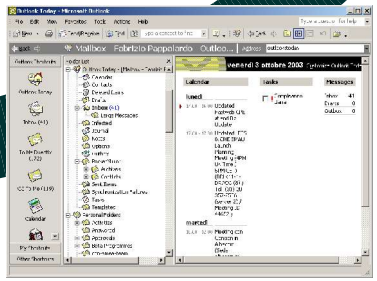
Instant Messaging





On line
Office supplies

Faxes

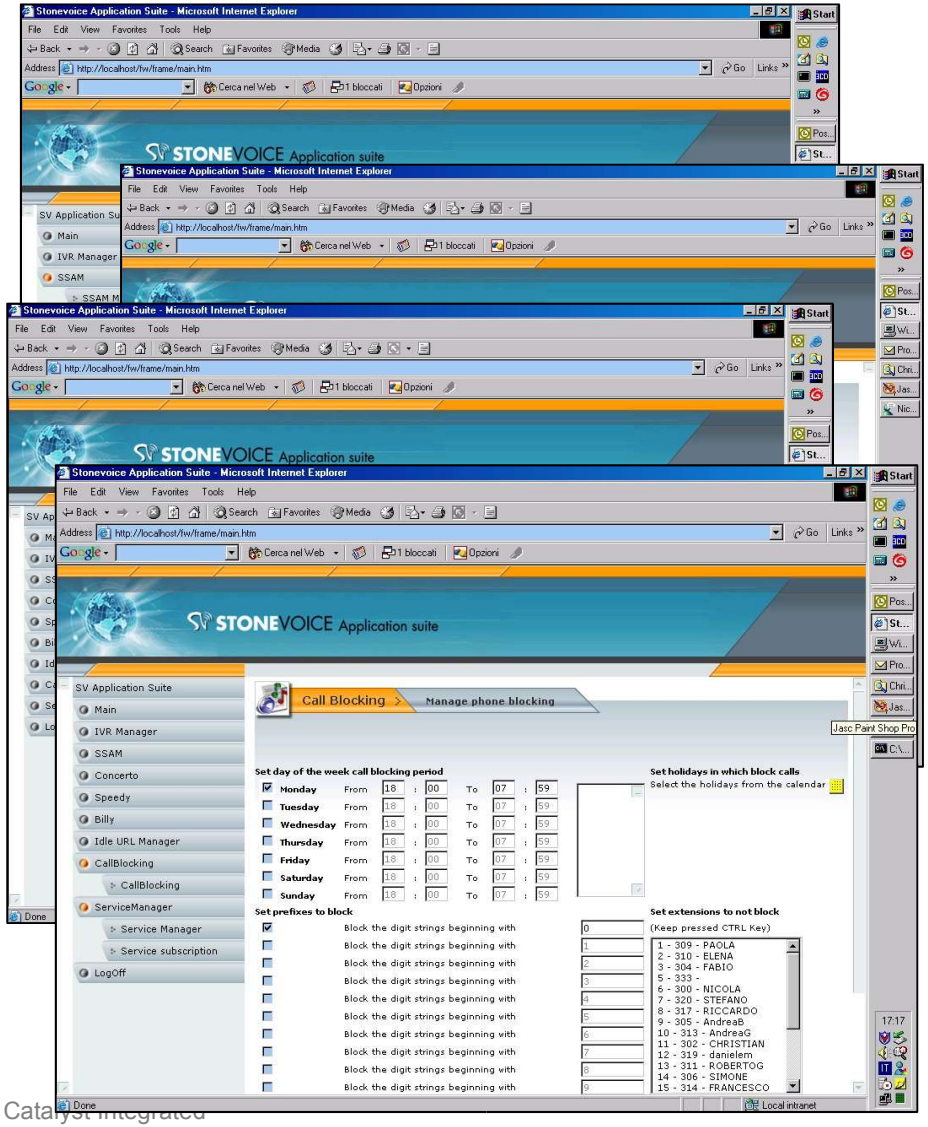


Email

Phone

© 2004 Cisco Systems, Inc. All rights reserved.

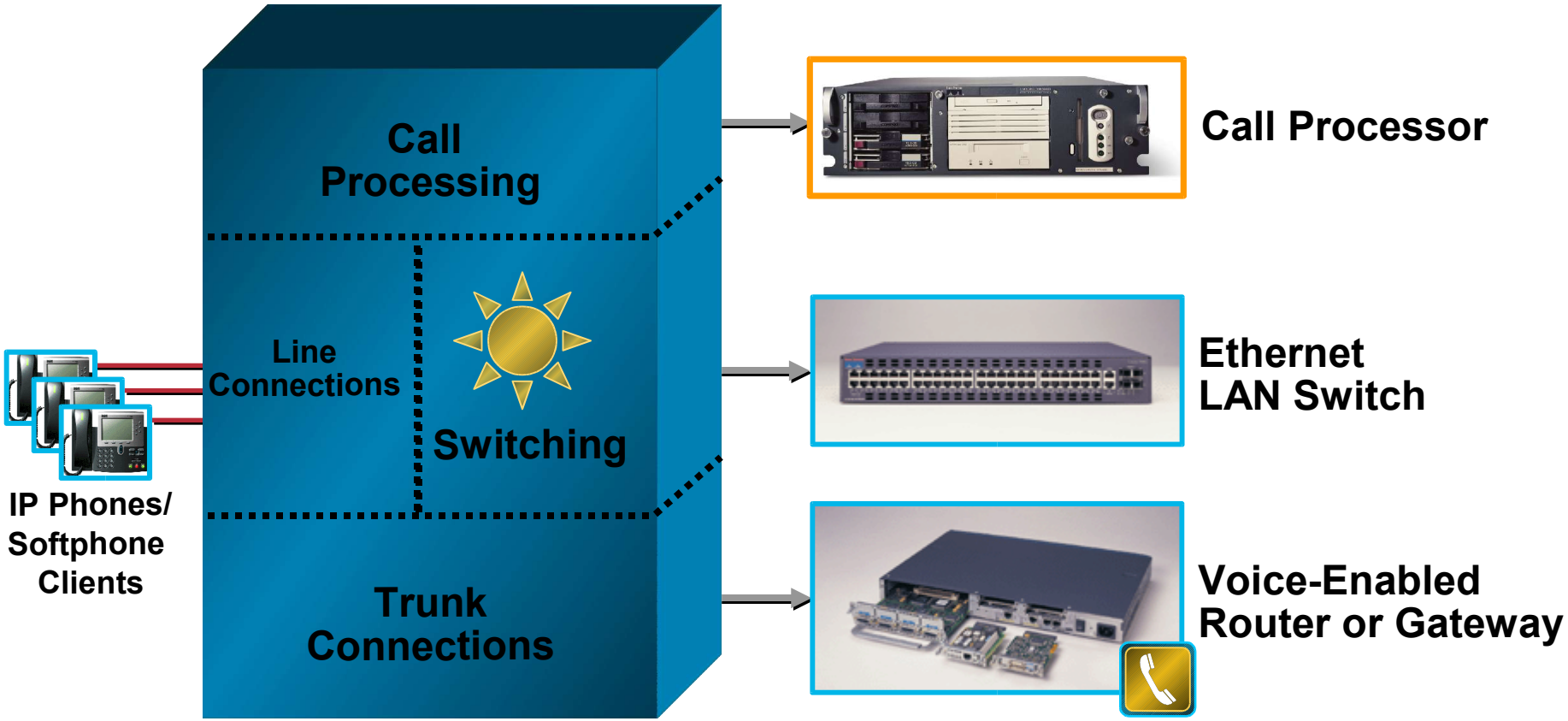
Small Offices that look big



© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

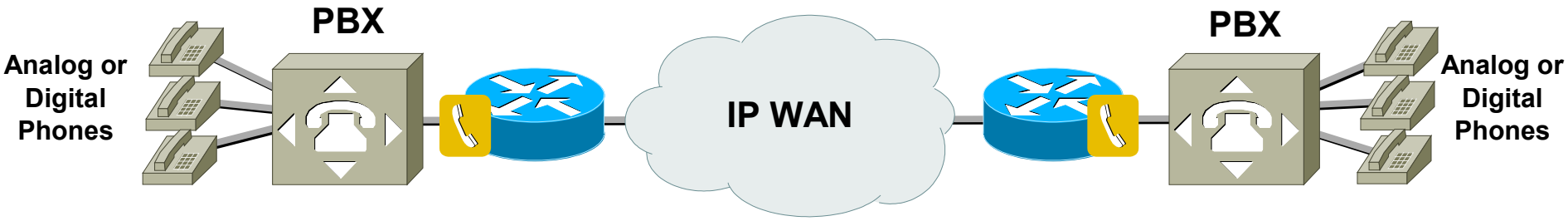
IP Telephony Building Blocks

IP Telephony distributes the PBX architecture

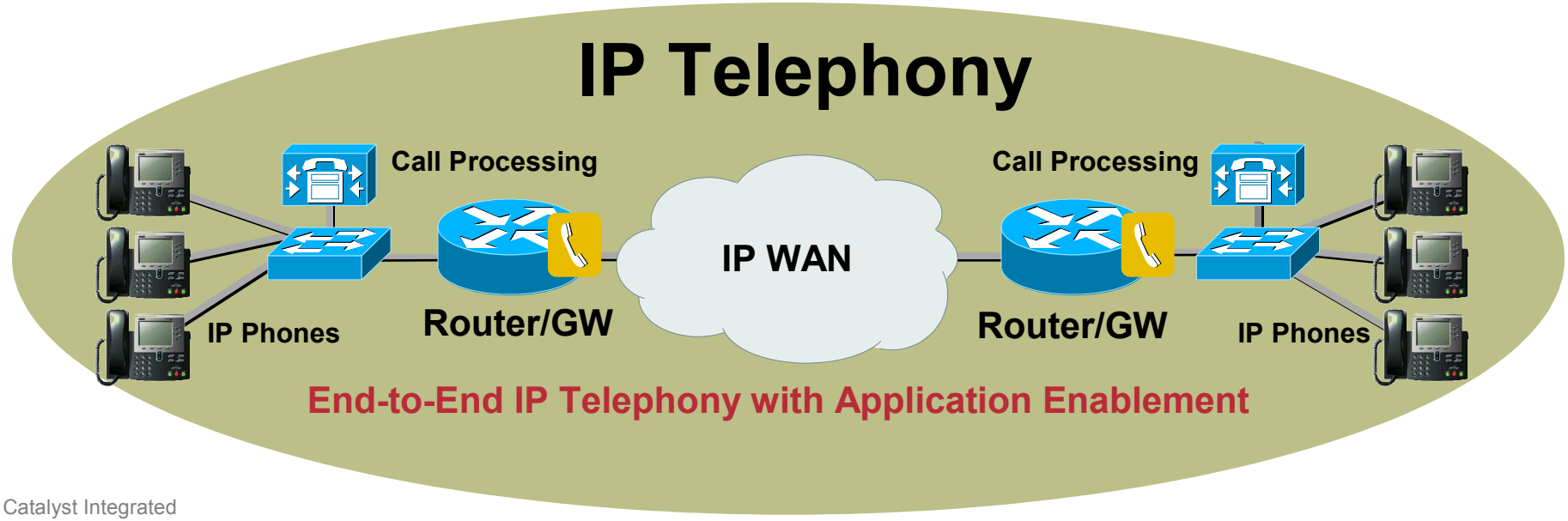


© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

‘VoIP’ Solution Sets:
Toll Bypass and IP Telephony

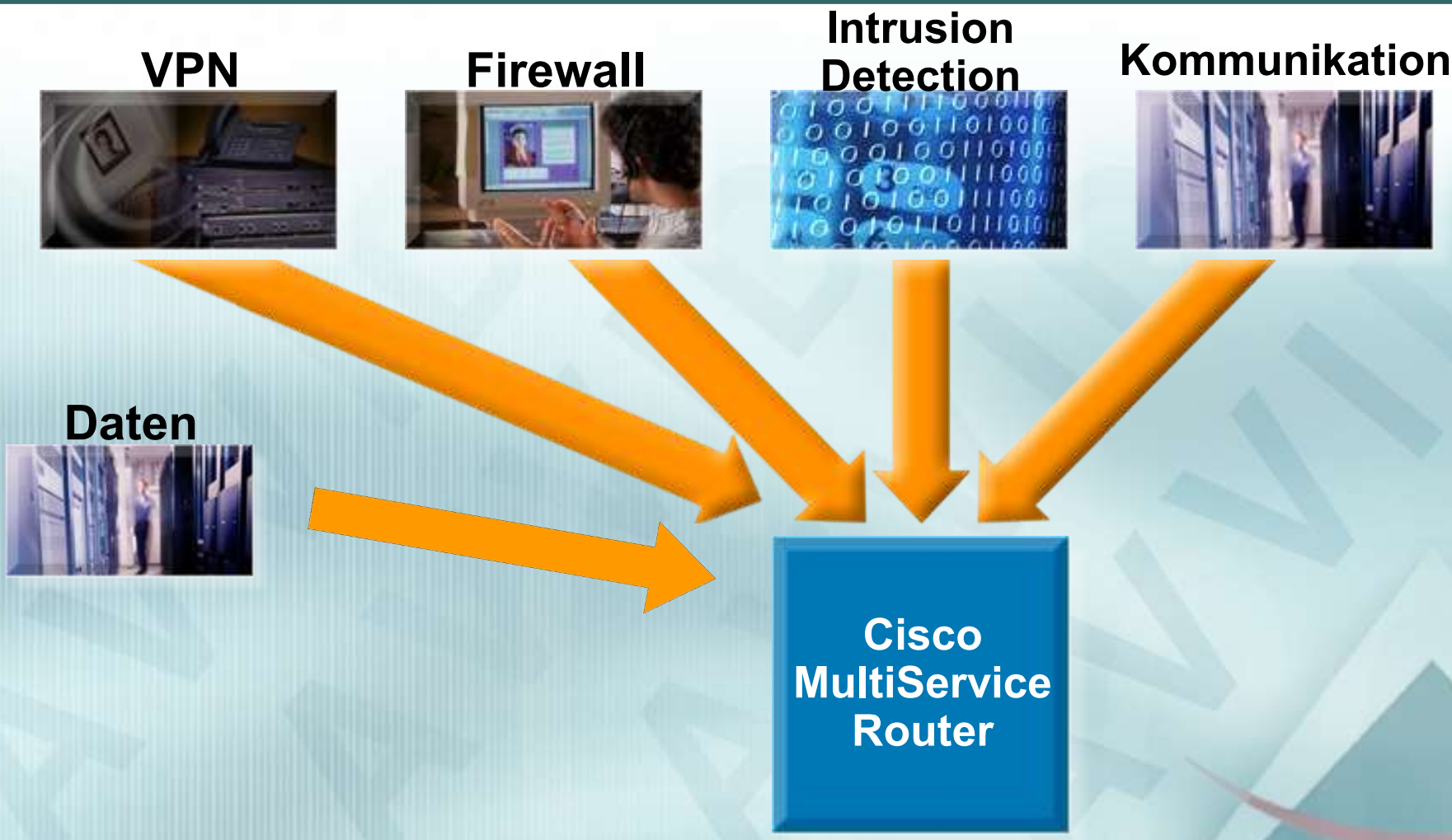


Toll Bypass



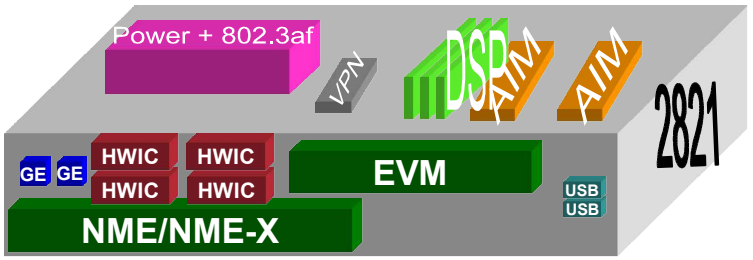
© 2004 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

All in ONE - Komplettlösung



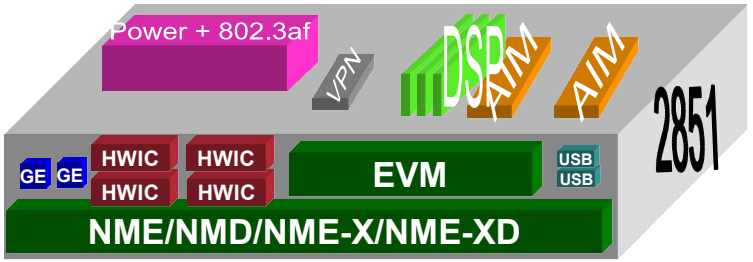
General Overview: 2800

2801



2821

2811



2851

	2801	2811	2821	2851
NME / EVM Slot	0 / 0	1 / 0	1 / 1	1 / 1
HWIC / VWIC Slots	2 / 2	2 / 4	2 / 4	2 / 4
Onboard DSP Slots	2	2	3	3
Onboard LAN	2FE	2 FE	2 GE	2 GE
Embedded IPSec (Mbps, IMIX)	14	20	30	50

© 2004 Cisco Systems, Inc. All rights reserved.

CME and SRST 3.2 Platform Density

Platform	CME 3.2		SRST 3.2		CUE
	Max. Phone	Max. DN	Max. Phone	Max. DN	
1751, 1760	24	120	24	120	No
2801	24	120	24	120	AIM Only
2811, 261xXM, 262xXM	36	144	36	144	AIM/NM
2821, 265xXM	48	144	48	192	AIM/NM
2691	72	288	72	288	AIM/NM
2851	96	288	96	288	AIM/NM
3725	144	500	144	576	AIM/NM
3745	192	500	480	960	AIM/NM
3825	168	500	336	960	AIM/NM
3845	240	720	720	960	AIM/NM

© 2004 Cisco Systems, Inc. All rights reserved.

Introducing Cisco Unity Express

- **Local Auto Attendant & Voice Mail system with 12-100 mailboxes, 4-8 sessions, 100 hours of storage**
- **Integrated in Cisco's Full Service Branch Routers**
  - **For the Small or Medium Branch Office (2600XM, 28XX, 3700, 3800)**
  - **Network Module (Release 1)**
- **Entry level Cisco Voice storage & processing products**

Key benefits:

- **Cost-effective** for the SMB or Branch
- **Application Integration** means fewer devices to manage - less staff support
- **Choice** of configurations and scale
- **Industry standard** closed, secure and embedded OS for voice mail

© 2004 Cisco Systems, Inc. All rights reserved.

"Will they need voice?"

Making Voice Services Sales Faster, Easier: Cisco 3800, 2800 IPC Bundles

V3PN Bundles	SRST Voice Bundles	CCME Voice Bundles	Entry Level Voice Bundles
3845-3VPN/K9	3845-SRST/K9	3845-CCME/K9	3845-V/K9
3825-3VPN/K9	3825-SRST/K9	3825-CCME/K9	3825-V/K9
2851-3VPN/K9	2851-SRST/K9	2851-CCME/K9	2851-V
2821-3VPN/K9	2821-SRST/K9	2821-CCME/K9	2821-V
2811-3VPN/K9	2811-SRST/K9	2811-CCME/K9	2811-V
2801-3VPN/K9	2801-SRST/K9	2801-CCME/K9	2801-V
Includes: Router, Cisco IOS Advanced Services, DSPs, AIM-VPN Accelerator	Includes: Router, Survivable Remote Site Telephony, Cisco IOS SP Services, DSPs, Memory	Includes: Router, Cisco CallManager Express, Cisco IOS SP Services, DSPs, Memory	Includes: Router, Cisco IOS SP Services, DSPs, Memory

© 2004 Cisco Systems, Inc. All rights reserved.

Making price comparisons

- **Do not compare only the HW + Installation costs:**

  Include maintenance, management, Installation fees

- **PBX Resellers applies 4 different costs:**

  HW, Installation&Design, Moves&Adds&Changes, Maintenance

© 2004 Cisco Systems, Inc. All rights reserved.

Sales Tool…

- TradeIn Mitbewerb TK Anlage: egal welche!!!
- TradeIn Cisco alt (Router) vs. Cisco neu (ISR Router)
- SMB Neukunden: Icebreaker Promo (Preissupport)
- PLUS -> OIP Programm (+6% von Listpreis)

© 2004 Cisco Systems, Inc. All rights reserved.

Q and A

© 2008 Cisco Systems, Inc. All rights reserved.

© 2003 Cisco Systems, Inc. All rights reserved.